Posudek oponenta bakalářské práce

Student: Jakubík Samuel
Téma: Útok na šifrování dokumentů OpenDocument s využitím GPU (id 19884)
Oponent: Čejka Rudolf, Ing., CVT FIT VUT

1. Náročnost zadání **obtížnější zadání**

Zadání považuji za obtížnější, jelikož se věnuje hned několika náročnějším oblastem současně, jako jsou algoritmy šifrování a hashování, práce s různými formáty dat a akcelerace výpočtů na GPU.

2. Splnění požadavků zadání **zadání splněno s drobnými výhradami**

Zadání bylo splněno, ale srovnání s konkurenčními nástroji v bodě 5 nepovažuji za dostatečné. Jeden nástroj nebyl testován vůbec, jelikož OpenDocument nepodporuje, a u druhého se nepodařila zprovoznit podpora GPU.

3. Rozsah technické zprávy **je v obvyklém rozmezí**

Práce odpovídá obvyklému rozsahu.

4. Prezentační úroveň předložené práce **60 b. (D)**

V teoretické části na sebe zcela nenavazují jednotlivé kapitoly. Nejdříve jsou bez zjevného důvodu zmiňovány hashovací funkce, pak šifrovací funkce, a až na konci další kapitoly o formátu OpenDocument je ukázáno, k čemu se používají. Dále bych více prostoru věnoval kapitolám o návrhu modulu a jeho implementaci.

5. Formální úprava technické zprávy **80 b. (B)**

Jazykovou stránku nedokážu plně posoudit, jelikož je psaná slovensky. Chybějící nebo nadbytečné čárky ve větách, překlepy a chybné tvary slov ale byly rozpoznatelné poměrně dobře (použitom šifrovaní súboru, polovicw dát a další).

6. Práce s literaturou **90 b. (A)**

K výběru studijních pramenů nemám zásadnější připomínky.

7. Realizační výstup **70 b. (C)**

Funkčnost byla pouze demonstrována, jelikož se projekt na jiném systému nepodařilo zprovoznit. Nutno ale podotknout, že problém v tomto případě není na straně studenta, ale spíše na straně rozšiřovaného nástroje Fitcrack/Wrathion, který například vyžaduje i historickou verzi jedné knihovny z roku 2013.

Změny a nové soubory student označil vcelku dobře, až na dva OpenCL soubory. U jednoho nejsou zřejmé provedené změny a u druhého je navíc odstraněn i původ.

8. Využitelnost výsledků

Výsledky práce budou zcela jistě využitelné v praxi, ale nejedná se o jedinou možnost, která existuje. A bohužel se nepodařilo ukázat, že by tato implementace měla být efektivnější než konkurence. Pokud se nepodaří zprovoznit AOPR s podporou GPU, doporučuji pro srovnání vyzkoušet John the Ripper s podporou OpenCL a OpenMP.

9. Otázky k obhajobě

- Na základě čeho se určuje, zda se bude při zkoušení různých hesel dešifrovat celý dokument, nebo jen jeho prvních 1024 bajtů?
- Jak funguje technologie HyperThreading a proč lze očekávat, že u výpočetně náročných úloh příliš nepomůže a někdy dokonce i uškodí?

10. Souhrnné hodnocení **70 b. dobře (C)**

Jako hodnocení navrhuji stupeň C, kde náročnější zadání vyvažuje zejména horší úroveň technické zprávy.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 3. června 2017

.....
podpis